APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/755,835	01/12/2004	Peter Daniel Birk	AUS920030095US1	9841

	EXAMINER
40412　　7590　　07/13/2007 IBM CORPORATION- AUSTIN (JVL) C/O VAN LEEUWEN & VAN LEEUWEN PO BOX 90609 AUSTIN, TX 78709-0609	ALMEIDA, DEVIN E

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
07/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)
	10/755,835	BIRK ET AL.
	Examiner	**Art Unit**	
	Devin Almeida	2132	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>23 May 2007</u>.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3, 6-14, 16-23 and 26-30* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3, 6-14, 16-23 and 26-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

This action is in response to the papers filed 5/23/2007. Claims 1-3, 6-14, 16-23, and 26-3 were received for consideration. Claims 4, 5, 15, 16, 24 and 25 were cancelled.

Response to Arguments

Applications arguments with respect to the rejection under 35 USC 101 are persuasive.

Applications arguments with respect to the rejection under 35 USC 112 to lack of antecedent basis are persuasive.

Applications arguments that neither Giles or Schneier teach "a domain, a maximum age, a path, a port, an authentication strength value, an authenticating server identifier, and an access control privilege identifier" is not persuasive. Giles teaches a global time out value valid for the whole domain which is usually a fixed offset added to the creation time; and a cookie inactivity time-out which is a fixed offset added to the cookie creation time (i.e. maximum age); and the domain name of the origin web-server (i.e. a domain).

Applications arguments that neither Giles or Schneier teach "creating an encrypting value based upon the access control data, wherein the creating comprises; hashing the access control data using a hashing algorithm, the hashing resulting in a hash value; and encrypting the hash value" is not persuasive. Giles teaches digital signing the access control date. Schneier teach that digital signatures protocols are often implemented with one-way hash functions in which, a function is applied to a

document to producing a one-way hash of a document (hash value). The hash (hash

value) is encrypted with a private key producing a digital signature of the document.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

Claims 9, 19 and 29 are rejected under 35 U.S.C. 112, second paragraph, as

being indefinite for failing to particularly point out and distinctly claim the subject matter

which applicant regards as the invention. Claim 9, 19 and 29 also are indefinite because

if the third computer system does not have access to the authentication data how is it

retrieving the authentication data from an authentication server and storing the

authentication data on a cache associated with the third computer.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Giles et al. (U.S. Patent # 6,986,047) in view of Schneier " Applied Crytography:

Protocols, Algorithms, and Source Code in C". Giles teaches with respect to claim 1 and

21, a method of handling client state information, said method comprising: receiving, at

a first computer system (see figure 3 element 310 origin web server), a first request

from a second computer system (see figure 3 element 305 Client), wherein the first

request is received over a computer network (see column 3 lines 36-51 and column 7

lines 10-62 i.e. a client sends a HTTP request); identifying access control data

pertaining to the second computer system (see figure 11 column 7 lines 10-62 i.e. the

origin web-server creates a valid cookie), the access control data includes a domain, a

maximum age, a path, a port, an authentication strength value, an authenticating server

identifier, and an access control privilege identifier (column 8 line 52 – column 9 line 8

i.e. a global time out value valid for the whole domain (1130) which is usually a fixed

offset added to the creation time; and a cookie inactivity time-out (1135) which is a fixed

offset added to the cookie creation time; and the domain name of the origin web-

server); creating an encrypted value based upon the access control data (see column 8

lines 52-66), wherein the creating comprises digital signing the access control date (i.e.

cookie) and encrypting the hash value (see column 8 line 52 – column 9 line 55 i.e. the

fields of the first part are encrypted using the key Kc); and storing, on the second

computer system, a state management data (see column 9 lines 11-12 i.e. the client

cookie may be present in the HTTP request by the client) structure that includes an

access control identifier (see column 8 line 66 – column 9 line 8) and the encrypted

value (see column 8 lines 52-66). Giles do not explicitly teach hashing the access

control data using a hashing algorithm. Schneier teaches that digital signatures

protocols are often implemented with one-way hash functions (Schneier page 38). It

would have been obvious at the time the invention was made to a person having

ordinary skill in the art to which said subject matter pertains to have use a digital

signature protocols that used a one-way hash functions to save time. Therefore one

would have be motivated to have used a use a digital signature protocols that used a

one-way hash functions to authenticate save and provide message integrity (Schneier

page 38).

With respect to 2, 12 and 22, authenticating a user of the second computer

system (see column 7 lines 10-62 i.e. user ID and password promt); and caching, on the

first computer system, security attributes of the authenticated user that are too sensitive

to be included in the state management data structure, wherein the cached security

attributes are indexed by the encrypted value and wherein cached security attributes

are adapted to re-establish a security context of the authenticated user (column 8 line

52 – column 9 line 8 i.e. the key kc shared by the semi-trusted web-server and the orgin

web-server).

With respect to 3, 13 and 23, wherein the access control identifier is selected

from the group consisting of the access control data (see column 8 line 52 – column 9

line 8 i.e. the access control identifier is the encrypted part of the access control data

(cookie)) and a unique identifier used by the first computer system to map to the access

control data stored on an authentication server (column 9 line 9 – column 9 line 55 i.e.

the cookie is decrypted by using the domain identifier and the key identifier to select an

appropriate decryption key).

With respect to 6, 16 and 26, storing the encrypted value at the first computer

system in response to receiving the first request (see column 7 line 10-62 i.e. at step

800 a client sends an HTTP request and after step 820 the orgin web-server creates a

cookie according to figure 11 and column 8 line 52 – column 9 line 8 this cookie is

digital signed and encrypted with key kc); receiving a second request from the second

computer system; retrieving the state management data structure from the second

computer system, the retrieving performed in conjunction with the reception of the

second request; and comparing the encrypted value included in the retrieved state

management data structure with the encrypted value stored at the first computer system

(column 9 line 9 – column 9 line 55).

With respect to 7, 17 and 27, re-establishing an authenticated user's security

context by using the encrypted value as a key to retrieve the access control data

cached on the first computer system (column 8 line 52 – column 9 line 55).

With respect to 8, 9, 18, 19, 28 and 29, authenticating a user of the second

computer system, wherein the identifying, creating, and storing are performed in

response to successfully authenticating the user (column 7 line 10-62).

With respect to 10, 20 and 30, receiving, at the first computer system, a second

request from the second computer system; retrieving the state management data

structure from the second computer system, the retrieving performed in conjunction with

the reception of the second request (column 9 line 9–55 i.e. process of validating a

client cookie and returning client credentials in case the cookie is valid as part of the

correlation procedures. The client cookie may be present in the HTTP request by the

client); determining that the retrieved state management data structure is stale based on

a timestamp included in the state management data structure (see column 9 line 11-55

i.e. at step 1210 the global time-out and inactivity time-out fields are checked); and

authenticating a user of the second computer system in response to the determination

(see column 9 line 11 – column 10 line 31).

     With respect to claim 11, a first information handling system comprising: one or

more processors; a memory accessible by the processors (see column 3 lines 36-51 i.e.

it is inherent that a computer has a processor and a memory); a network interface

connecting the information handling system to a computer network (see column 3 lines

36-51); a tool for handling client state information, the tool including software effective to

(see column 4 lines 21-41): receiving, at a first computer system (see figure 3 element

310 origin web server), a first request from a second computer system (see figure 3

element 305 Client), wherein the first request is received over a computer network (see

column 3 lines 36-51 and column 7 lines 10-62 i.e. a client sends a HTTP request);

identifying access control data pertaining to the second computer system (see column 7

lines 10-62 and column 8 line 52 – column 9); creating an encrypted value based upon

the access control data (see column 8 line 52 – column 9 line 55 i.e. key kc); and

storing, on the second computer system, a state management data (i.e. cookie)

structure that includes an access control identifier and the encrypted value (see column

7 lines 10-62 and column 8 line 52 – column 9 line 55 i.e. the client cookie may be

present in the HTTP request by the client).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Devin Almeida whose telephone number is 571-270-

1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to

5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to

4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

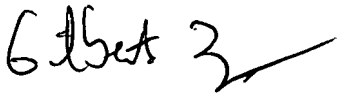published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Devin Almeida
Patent Examiner
7/5/2007

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100